UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

BLACK SAMSUNG SMARTPHONE WITH IMEI NUMBER 353339110444341 AT ATF EVIDENCE ROOM, 08-491, 550 MAIN ST. CINTI, OH 45202

Case No. 1:20-mj-729

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Souterhn District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 922(g)(1)	Possession by a Prohibited Person

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Nicholas S Radebaugh
Applicant's signature

Nicholas Radebaugh, Special Agent ATF
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by FaceTime video *(specify reliable electronic means).*

Date: 10/13/2020

Karen L. Litkovitz
Judge's signature

City and state: Cincinnati, Ohio

Hon. Karen L. Litkovitz, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

The property to be searched is a black Samsung smartphone, with IMEI number 353339110444341. The device is currently located in the ATF Evidence Room at 550 Main Street, Cincinnati, Ohio, Room 8-491.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 922(g)(1) and involve Daniel AMBROSE since July 1, 2020 including:

a. any communications, including but not limited to: phone calls, text messages, application messages, relating to sources of and possession of firearms;

b. any information related to sources of firearms (including names, addresses, phone numbers, or any other identifying information);

c. any internet search history and browser files related to sources and possession of firearms;

d. types and amounts of firearms possessed as well as dates, places, and amounts of specific firearms transactions;

e. any information, including GPS location information, recording AMBROSE's schedule or travel from July 1, 2020 to August 10, 2020;

f. any photographs and videos, including metadata, and any other records, relating to source or possession of firearms; and

g. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT
FOR SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF CELLULAR TELEPHONES DESCRIBED AS: A WHITE LG SMARTPHONE, WITH IMEI NUMBER 356284106706658 A BLACK SAMSUNG SMARTPHONE, WITH IMEI NUMBER 353339110444341 **LOCATED AT THE ATF EVIDENCE ROOM**, 08-491 FEDERAL BUILDING, 550 MAIN STREET, CINCINNATI, OHIO 45505	**CASE NO.** 1:20-mj-729 **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Nicholas Radebaugh, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment A.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and have been so employed since May of 2018. As a part of my training with

the ATF, I graduated from the Federal Law Enforcement Training Center (FLETC), Criminal Investigator School, located in Glynco, Georgia. I also graduated from the ATF Special Agent Basic Training Academy, located in Glynco, Georgia, on November 15th, 2018. I am currently assigned to an Organized Crime Task Force which investigates criminal organizations in the Southern Judicial District of Ohio. Prior to my employment with ATF, I was a Federal Air Marshal with the Department of Homeland Security in New York, NY for six years. From 2008 to 2011, I was a member of the Orlando Police Department, where I served as a patrol officer in the Bravo District of Orlando. I am an Army veteran with the 82nd Air Borne Division, where I served as a Counter Intelligence Agent, and I hold a Bachelor's of Science Degree in Criminal Justice from Grand Valley State University, located in Grand Rapids, MI. In addition to graduating from the ATF academy, I have also graduated from Uniform Police Training Program FLETC academy, City of Orlando Police Academy, and the Federal Air Marshal FLETC academy.

3. This affidavit is submitted in support of an application for a federal search warrant for the following devices as there is probable cause to believe that evidence of a crime-namely, violations of 18 U.S.C. § 922(g)(1) (Possession by a Prohibited Person). This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is:

- A WHITE LG SMARTPHONE, WITH IMEI NUMBER 356284106706658
- A BLACK SAMSUNG SMARTPHONE, WITH IMEI NUMBER 353339110444341

hereinafter referred to as the "Devices." The Devices are currently located at the ATF Cincinnati Field Office, located at 8-491 Federal Building, 550 Main Street, Cincinnati, Ohio 45505.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On August 10, 2020, Cincinnati Police Department (CPD) officers were conducting surveillance in the area of 1215 Neff Street, Cincinnati, Ohio 45204, located in the Southern District of Ohio. The residence is owned by Daniel AMBROSE and records checks confirm the residence is AMBROSE's current address. CPD officers were conducting surveillance at 1215 Neff Street because AMBROSE and his associates were suspects in several recent shooting incidents in the Avondale neighborhood.

7. During surveillance, Officer Broering saw AMBROSE exit the front passenger side door of a 2012 maroon KIA Optima, bearing Ohio temporary tag L474763. Once outside of the vehicle, Officer Broering saw AMBROSE in possession of a suspected firearm, which AMBROSE was holding in his right hand. Officer Broering described the firearm as a black, thin, semiautomatic style pistol. After exiting the vehicle, AMBROSE went into the residence with the firearm.

8. After several minutes, CPD officers saw AMBROSE and Wesley NOBLE exit the residence and get into a 2011 white Jeep Liberty, bearing Ohio license plate HRM5086. Uniformed officers responded to the area and witnessed the NOBLE, the driver of the Jeep Liberty, commit a traffic violation. Uniformed officers initiated a traffic stop on the vehicle in the area of 1400 Gest Street, Cincinnati, Ohio, located in the Southern District of Ohio. As CPD

officers approached the vehicle, they could see the passenger, later identified as AMBROSE, moving around the cab of the passenger side of the vehicle.

9. During a subsequent search of the vehicle, CPD officers found two firearms, a Taurus, model PT709 slim, 9 millimeter caliber semiautomatic handgun bearing serial number TEZ14834 and a Smith and Wesson, model SD40, .40 caliber semiautomatic firearm bearing serial number FBM4356. Both firearms were recovered from behind the glove box on the passenger side of vehicle where AMBROSE was seated. Officer Broering identified the Taurus as the firearm he saw AMBROSE carrying earlier that day.

10. Both AMBROSE and NOBLE were arrested and charged in Hamilton County (OH) Court of Common Pleas in reference to multiple firearm offenses in violation of Ohio law.

11. During a search incident to arrest, officers found a black Samsung smartphone, bearing IMEI number 353339110444341 on NOBLE's person; and a white LG smartphone bearing IMEI number 356284106706658 on AMBROSE's person.

12. On September 14, 2020, I reviewed information on NOBLE's Facebook account. From my review, I learned Wesley NOBLE's Facebook account was using Account Vanity Name ID: wesley.b.noble and User ID: 100001559578814. Based on NOBLE's public setting, I viewed photos and videos publically posted to NOBLE's account.

13. NOBLE publically posted multiple "live videos" which were saved in the video section of his Facebook account. These videos can be viewed by users with a Facebook account, but were publically posted. I watched multiple videos NOBLE posted and saw both NOBLE and AMBROSE possessing suspected firearms. These videos appear to be filmed by cell phone device. In one video posted on July 1, 2020, which is approximately three minutes and three seconds long, NOBLE and AMBROSE are driving in a vehicle. AMBROSE is riding as a

passenger. During the video, AMBROSE and NOBLE discuss selling a "XD 20" firearm to an individual on the live video feed. Approximately two minutes into the video, both AMBROSE and NOBLE show firearms to the camera. Multiple videos on NOBLES' Facebook account show AMBROSE using and operating a cell phone.

14. Through the course of the investigation, I learned AMBROSE uses a Facebook account. AMBORSE has communicated with NOBLE, using the Facebook Vanity Name: daniel.ambrose and User ID:100007160492406. AMBROSE and NOBLE sent messages, videos, and photographs between their two accounts as recent as July 2020. Based on my training and experience, I know that individuals often use Facebook and Facebook Messenger through installed applications on their cellular devices.

15. A records check confirmed AMBROSE had previously been convicted of a felony aggravated trafficking in drugs offense in Hamilton County (OH) Court of Common Pleas case number B1600856, which is punishable by a term of imprisonment exceeding one year. As such, AMBROSE was prohibited from possessing firearms at the time of his August 10, 2020 arrest.

16. Based on my training and experience in investigating firearm violations and firearms trafficking, I know that individuals routinely utilize their cell phones in furtherance of their firearm possession. Specifically, firearm possessors and traffickers discuss business arrangements via text message, email, social media and other means of communication. These individuals also often photograph themselves with firearms. These photographs are then stored and maintained on their cell phones.

17. Based upon my training and experience; the fact that AMBROSE and NOBLE were arrested carrying the described Devices; the fact that NOBLE used a cellular device to take videos of AMBROSE possessing firearms; the fact that AMBROSE is on video carrying a

cellular device while possessing firearms; the fact that AMBROSE has a Facebook account and has communicated with NOBLE using Facebook messenger, I believe that the Devices will contain evidence of AMBROSE's illegal possession of firearms in violation of 18 U.S.C. § 922(g)(1) (Possession by a Prohibited Person).

18. The Devices are currently in the lawful possession of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and are currently in storage at the ATF, located at 8-491 Federal Building, 550 Main Street, Cincinnati, Ohio 45505. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the Bureau of Alcohol, Tobacco, Firearms and Explosives.

19. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence of a crime - namely, Title 18 U.S.C. § 922(g)(1) – Possession by a Prohibited Person, which prohibits the possession of a firearm by a prohibited person - exists and can be found within the a black in color, Samsung smartphone, bearing IMEI number 353339110444341 and the white in color, LG smartphone, bearing IMEI number 356284106706658, located at the ATF, 8-491 Federal Building, 550 Main Street, Cincinnati, Ohio 45505.

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of

transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video,

or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication

devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, which is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control

a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

21. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as "a wireless telephone, digital camera, portable media player, GPS navigation device, PDA and Tablet." In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

23. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

24. *Forensic evidence.* As further described in Attachment A, this application seeks permission to locate not only electronically stored information that might serve as direct

evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

27. Based on the above facts and circumstances, I submit that this affidavit supports probable cause for a search warrant authorization the examination of the Device described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

28. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this

investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Nicholas S Radebaugh
NICHOLAS RADEBAUGH
Special Agent, Bureau of Alcohol,
Tobacco, Firearms, and Explosives

Subscribed and sworn to me this 13 day of October, 2020.

Karen L. Litkovitz
KAREN L. LITKOVITZ
UNITED STATES MAGISTRATE JUDGE